



Docker: Лучшие практики



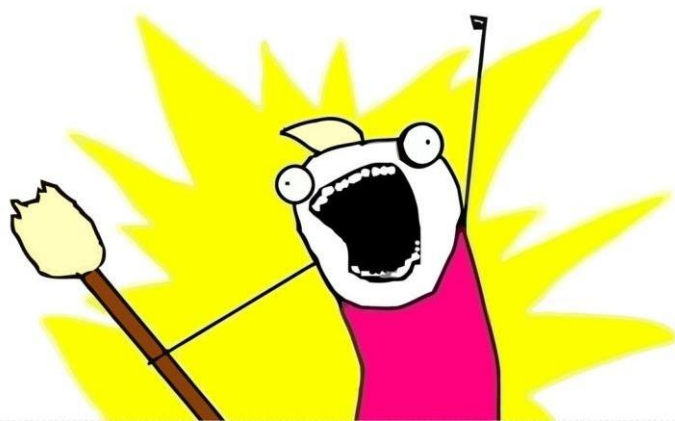
Что будем делать:

- Узнаем best practice по работе с Docker
- Узнаем как делать не нужно
- Поработаем самостоятельно



Чего мы хотим?

- Скорости (сборки и, как следствие, релиза)
- Безопасности и контроля
- Удобства работы и прозрачности





Ускоряемся...

- Тюнинг Dockerfile
- .dockerignore
- Размер образа
- Кеширование
- Multi-stage сборка



image: docker:19.03.1

services:

- docker:19.03.1-dind

variables:

Use TLS https://docs.gitlab.com/ee/ci/docker/using_docker_build.html#tls-enabled

DOCKER_HOST:tcp://docker:2376

DOCKER_TLS_CERTDIR: "/certs"

before_script:

- docker login -u \$CI_REGISTRY_USER -p \$CI_REGISTRY_PASSWORD \$

build:

stage: build

script:

- docker pull \$CI_REGISTRY_IMAGE:latest || true
- docker build --cache-from \$CI_REGISTRY_IMAGE:latest --tag \$CI_REGISTRY_IMAGE:\$CI_COMMIT_SHA --tag \$CI_REGISTRY_IMAGE:latest .
- docker push \$CI_REGISTRY_IMAGE:\$CI_COMMIT_SHA
- docker push \$CI_REGISTRY_IMAGE:latest

FROM golang:1.11-alpine AS build

Install tools required for project

Run 'docker build --no-cache .' to update dependencies

RUN apk add --no-cache git

RUN go get github.com/golang/dep/cmd/dep

List project dependencies with Gopkg.toml and Gopkg.lock

These layers are only re-built when Gopkg files are updated

COPY Gopkg.lock Gopkg.toml /go/src/project/

WORKDIR /go/src/project/

Install library dependencies

RUN dep ensure --vendor-only

Copy the entire project and build it

This layer is rebuilt when a file changes in the project directory

COPY . /go/src/project/

RUN go build -o /bin/project

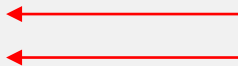
This results in a single layer image

FROM scratch

COPY --from=build /bin/project /bin/project

ENTRYPOINT ["/bin/project"]

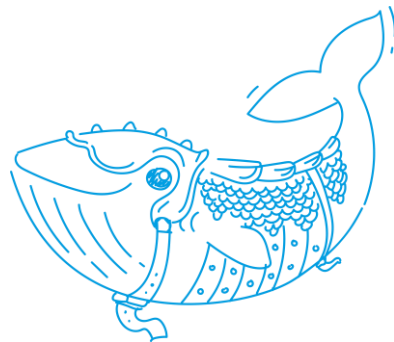
CMD ["--help"]






Усиливаем контроль и безопасность

- Не используем latest!
- Указываем явные версии ПО
- 1 процесс – 1 контейнер
- The Twelve-factor App
- Метрики и логи приложения
- Настройка приложения через env
- Resource management
- Минимум привилегий процесса в контейнере (mount, host network, root..)
- Свой базовый образ || тестим образы на уязвимости (<https://snyk.io>)





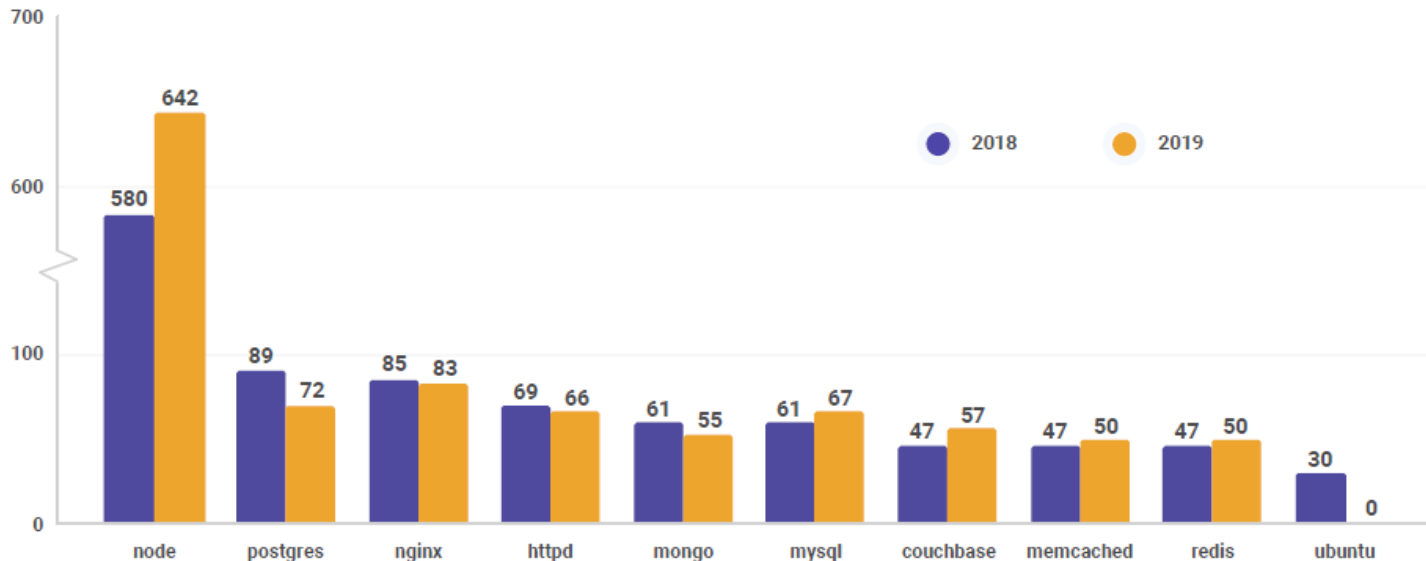
Сколько всего уязвимостей нашли в
популярных образах с Docker Hub?

 Start presenting to display the poll results on this slide.



Number of OS vulnerabilities by docker image

Vulnerabilities in official container images





Audience Q&A Session

 Start presenting to display the audience questions on this slide.



southbridge.io

Спасибо!

СЛЁРМ

slurm.io